

SYSTEM AND METHOD FOR INFORMATION TRANSACTION AND PROGRAM SUPPLY MEDIUM

Publication number: JP2001230768 (A)

Publication date: 2001-08-24

Inventor(s): ISHIBASHI YOSHITO; SHIRAI TAIZO

Applicant(s): SONY CORP

Classification:

- international: G09C1/00; G06F12/14; G06F21/00; G06F21/24; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G07F7/08; G07F17/00; G11B20/00; H04L9/08; H04L9/32; H04L29/06; G09C1/00; G06F12/14; G06F21/00; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; G07F7/08; G07F17/00; G11B20/00; H04L9/08; H04L9/32; H04L29/06; (IPC1-7): H04L9/08; G06F12/14; G06F15/00; G06F17/60; G07F7/08; G07F17/00; G09C1/00; H04L9/32

- European: H04L29/06S12A; G06Q20/00; G06Q20/00K2B; G11B20/00P; H04L29/06S4B2; H04L29/06S4B8

Application number: JP20000036353 20000215

Priority number(s): JP20000036353 20000215

Also published as:

US2002138733 (A1)

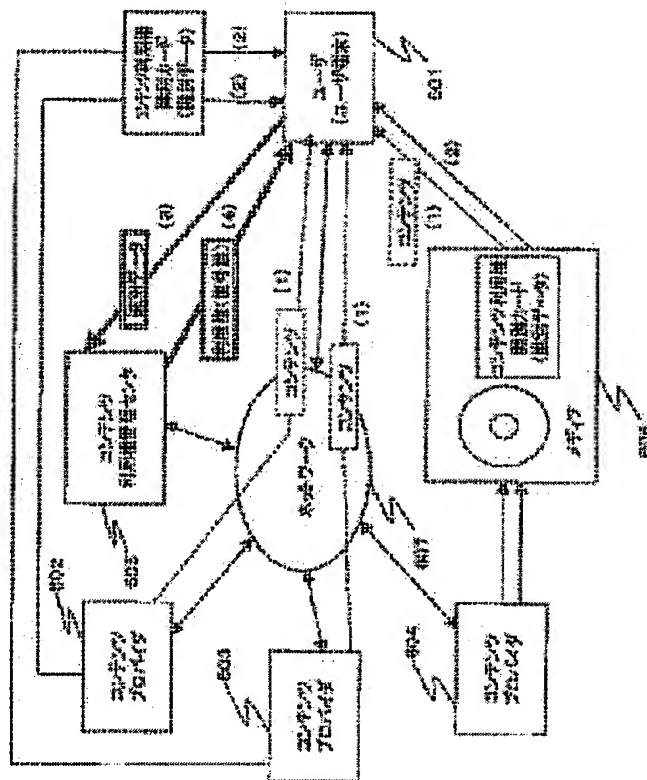
US7124443 (B2)

WO0161911 (A1)

Abstract of JP 2001230768 (A)

PROBLEM TO BE SOLVED: To provide an information transaction system and an information transaction method, which enable contents to be used without conducting a settlement by online.

SOLUTION: A contents use right identification card corresponding to ciphered contents is sold to a user. The user transmits data recorded in the content use right identification card to a contents use right management center. The contents use right management center identifies the contents and the card based on data of the received contents use right identification card, ciphers a contents key for contents decoding by a session key, for example, and transmits it to the user. The contents use right identification card sold to the user can be set so that it can be reprinted and transferred between the users. Thus, the contents key can be transmitted from the contents use right management center for plural times.



Data supplied from the esp@cenet database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-230768
(P2001-230768A)

(43) 公開日 平成13年8月24日 (2001.8.24)

(51) Int.Cl. ⁷	識別記号	F I	ターミナル* (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 E 3 E 0 4 4
G 0 6 F 12/14	3 2 0	15/00	3 3 0 Z 5 B 0 1 7
15/00	3 3 0	G 0 7 F 17/00	B 5 B 0 4 9
17/60	Z E C	G 0 9 C 1/00	6 2 0 Z 5 B 0 8 5
			6 4 0 Z 5 J 1 0 4

審査請求 未請求 請求項の数36 O L (全 26 頁) 最終頁に続く

(21) 出願番号 特願2000-36353(P2000-36353)

(22) 出願日 平成12年2月15日 (2000.2.15)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 白井 太三

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

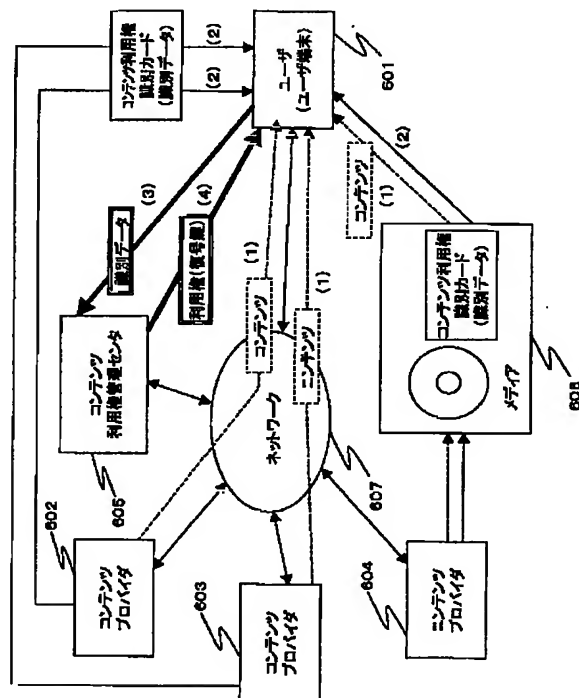
最終頁に続く

(54) 【発明の名称】 情報取り引きシステムおよび情報取り引き方法、並びにプログラム提供媒体

(57) 【要約】

【課題】 コンテンツの利用をオンラインでの決済処理を実行することなく利用可能とする情報取り引きシステムおよび情報取り引き方法を提供する。

【解決手段】 暗号化コンテンツに対応するコンテンツ利用権識別カードをユーザに販売し、ユーザはコンテンツ利用権識別カードに記録されたデータをコンテンツ利用権管理センタに送信する。コンテンツ利用権管理センタは受信したコンテンツ利用権識別カードのデータに基づいてコンテンツおよびカードを識別して、コンテンツ復号用のコンテンツ鍵をユーザに、例えばセッション鍵で暗号化して送信する。ユーザに対して販売されるコンテンツ利用権識別カードは、再販可能とする設定が可能であり、ユーザ間で譲渡することによって複数回、コンテンツ利用権管理センタからコンテンツ鍵の送信を受けることができる。



【特許請求の範囲】

【請求項1】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有し、前記ユーザ機器は、通信手段または記憶媒体メディアを介して取得した暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記通信手段を介して前記コンテンツ利用権管理手段に送信する構成を有し、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信する構成を有することを特徴とする情報取り引きシステム。

【請求項2】前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成を有することを特徴とする請求項1に記載の情報取り引きシステム。

【請求項3】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させる構成としたことを特徴とする請求項1に記載の情報取り引きシステム。

【請求項4】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式としたことを特徴とする請求項1に記載の情報取り引きシステム。

【請求項5】前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供する構成としたことを特徴とする請求項1に記載の情報取り引きシステム。

【請求項6】前記コンテンツ利用権管理手段は、前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信する構成を有することを特徴とする請求項1に記載の情報取り引きシステム。

【請求項7】前記コンテンツ利用権管理手段は、

同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供する構成を有し、

前記データベースには、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定した構成を有することを特徴とする請求項6に記載の情報取り引きシステム。

【請求項8】前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売する構成としたことを特徴とする請求項7に記載の情報取り引きシステム。

【請求項9】前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供回数を記録する構成を有することを特徴とする請求項7に記載の情報取り引きシステム。

【請求項10】前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントする構成を有することを特徴とする請求項6に記載の情報取り引きシステム。

【請求項11】前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定する構成としたことを特徴とする請求項10に記載の情報取り引きシステム。

【請求項12】前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定する構成を有することを特徴とする請求項6に記載の情報取り引きシステム。

【請求項13】前記コンテンツ利用権識別カードは、コンテンツ識別データ、コンテンツ利用権識別カードのカード識別データ、およびコンテンツ利用権識別カード中のデータの改竄を検証するためのチェックデータを含むことを特徴とする請求項1に記載の情報取り引きシステム。

【請求項14】前記チェックデータは、コンテンツ利用権識別カードを発行または管理する機関による電子署名データであることを特徴とする請求項13に記載の情報取り引きシステム。

【請求項15】前記コンテンツ利用権識別カードのカード識別データは、コンテンツ利用権識別カードの流通経路を判別可能なカード識別データであることを特徴とする請求項13に記載の情報取り引きシステム。

【請求項16】前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定する構成であることを特徴とする請求項13に記載の情報取り引きシステム。

【請求項17】前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信する構成であることを特徴とする請求項1に記載の情報取り引きシステム。

【請求項18】前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信する構成であることを特徴とする請求項1に記載の情報取り引きシステム。

【請求項19】前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信する構成であることを特徴とする請求項1に記載の情報取り引きシステム。

【請求項20】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有する情報取り引きシステムにおける情報取り引き方法において、暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、前記コンテンツ利用権管理手段において、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信するステップと、を有することを特徴とする情報取り引き方法。

【請求項21】前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得することを特徴とする請求項20に記載の情報取り引き方法。

【請求項22】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させること

を特徴とする請求項20に記載の情報取り引き方法。

【請求項23】前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式であることを特徴とする請求項20に記載の情報取り引き方法。

【請求項24】前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供することを特徴とする請求項20に記載の情報取り引き方法。

【請求項25】前記コンテンツ利用権管理手段は、前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信することを特徴とする請求項20に記載の情報取り引き方法。

【請求項26】前記コンテンツ利用権管理手段は、同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供し、前記データベースに、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定することを特徴とする請求項25に記載の情報取り引き方法。

【請求項27】前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売することを特徴とする請求項26に記載の情報取り引き方法。

【請求項28】前記コンテンツ利用権管理手段は、前記データベースに、前記コンテンツ利用権識別カード毎のコンテンツ鍵の提供回数を記録することを特徴とする請求項26に記載の情報取り引き方法。

【請求項29】前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、

前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントすることを特徴とする請求項25に記載の情報取り引き方法。

【請求項30】前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定することを特徴とする請求項29に記載の情報取り引き方法。

【請求項31】前記コンテンツ利用権管理手段の前記データベースは、

前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、

前記コンテンツ利用権管理手段は、

前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定することを特徴とする請求項25に記載の情報取り引き方法。

【請求項32】前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定することを特徴とする請求項20に記載の情報取り引き方法。

【請求項33】前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信することを特徴とする請求項20に記載の情報取り引き方法。

【請求項34】前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信することを特徴とする請求項20に記載の情報取り引き方法。

【請求項35】前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信することを特徴とする請求項20に記載の情報取り引き方法。

【請求項36】コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器におけるコンテンツ情報取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

オフラインでユーザに提供されるコンテンツ利用権識別カードに記録されたコンテンツ利用権識別データを前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、

前記コンテンツ利用権管理手段から受信したコンテンツ鍵に基づいて暗号化コンテンツを復号処理するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報取り引きシステムおよび情報取り引き方法、並びにプログラム提供媒体に関する。特に、音楽、画像データ、ゲームプログラム等の各種コンテンツ情報をCD、DVD等の記録媒体を介して、あるいはネットワークを介した配信によりユー

ザに提供し、ユーザからコンテンツ利用に伴う利用料金の回収あるいは利用ポイントの付与等を実行する構成を有する情報取り引きシステムおよび情報取り引き方法に関する。

【0002】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体（メディア）を介して流通している。これらの流通コンテンツは、一般にユーザの所有するPC（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモ리카ード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。

【0003】従来のビデオゲーム機器、PC等の情報機器において使用されるメモ리카ード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモ리카ードに備えられた不揮発性メモリはEEPROM、フラッシュメモリ等によって構成される。

【0004】DVD、CD等の流通可能な記憶媒体（メディア）、あるいはメモ리카ード等の記憶手段に記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により各記憶手段から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0005】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、コンテンツの配布時、すなわちコンテンツがDVD、CD等の記憶媒体によって流通する場合には、DVD、CD等の記憶媒体の販売時に代金を回収したり、あるいはインターネット等のネットワークを介してコンテンツを配信する場合には、コンテンツ配信に際してユーザのクレジット番号等のユーザ情報を取得してユーザからコンテンツ提供に対する対価、すなわち利用料金を取得する構成を採用している。

【0006】これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないよう、セキュリティを考慮した構成をとるのが一般的となっており、DVD、CD等の記憶媒体（メディア）、あるいはネットワークを介したコンテンツデータの配信においては、配布コンテンツを暗号化して、正規

なユーザであると確認された場合にのみ、暗号化コンテンツを復号可能な鍵（コンテンツ鍵）を提供する構成が採用されている。

【0007】例えば、昨今のデジタルデータ（コンテンツ）のオンライン販売システムの構成としては、ユーザがネットワークやメディア経由で暗号化されたコンテンツを取得し、コンテンツを利用するために、ユーザ端末をコンテンツ利用権販売センターに接続してコンテンツの利用権購入手続きをオンラインで行ない、暗号化コンテンツの復号処理に適用する鍵をネットワークを介して取得する態様が普及しつつある。

【0008】暗号化されたコンテンツデータは、オンライン手続きによってコンテンツ利用権販売センターから取得した鍵を用いて復号化処理が可能となり、復号処理によってユーザ端末において利用可能な復号データ（平文）に戻ることができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0009】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0010】上述の暗号化処理、復号化処理に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方方向性関数を適用して得ることができる。一方方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【0011】また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が配布した公開鍵または認証局から入手した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を配布した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号す

ることができる。公開鍵暗号化方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。

【0012】このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図1を用いて簡単に説明する。

【0013】図1は、PC（パーソナルコンピュータ）、ゲーム機器等の再生手段10において、DVD、CD30、インターネット40等のデータ提供手段から取得したプログラム、音声データ、映像データ等（コンテンツ（Content））を再生するとともに、DVD、CD30、インターネット40等から取得したデータをフロッピーディスク、メモ리카ード、ハードディスク等の記憶手段20に記憶可能とした構成例を示すものである。

【0014】プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段10を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。

【0015】再生手段10はCPU12を有し、入力データの再生処理を再生処理部14で実行する。再生処理部14は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

【0016】正規ユーザは、提供されたプログラムを、再度使用するために記憶手段20にプログラム／データ等、コンテンツの保存処理を行なう。再生手段10には、このコンテンツ保存処理を実行するための保存処理部13を有する。保存処理部13は、記憶手段20に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。

【0017】コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部13は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをFD（フロッピーディスク）、メモ리카ード、ハードディスク等の記憶手段20の記憶部21に記憶する。

【0018】ユーザは、記憶手段20から格納コンテンツを取り出して再生する場合には、記憶手段20から、暗号化データを取り出して、再生手段10の再生処理部14において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

【0019】

【発明が解決しようとする課題】このような暗号化コンテンツの利用には、前述したようにコンテンツ利用権販売センタからコンテンツの正規利用権を取得し、暗号化コンテンツの復号処理に適用する鍵を購入することが必要となるが、この購入代金の支払いの方法としては、例

例えば(1)クレジットカード番号を端末から入力してコンテンツ利用権販売センタに送信する。(2)ユーザの銀行口座番号を端末から入力してコンテンツ利用権販売センタに送信する。(3)予めコンテンツ利用権販売センタにユーザ登録を行ない、クレジットカード番号、あるいは銀行口座番号を登録し、コンテンツ利用権販売センタが登録済みデータに基づいて引き落としを実行する。(4)電子マネーを利用する。これらの各種の方法がある。

【0020】しかしながら、これら(1)～(3)の支払方法においてはユーザのクレジットカード番号、あるいは銀行口座番号が要求されることになる。従って、これらのクレジットカード、銀行口座を持たない例えば未成年者にとっては、この支払い手続きが困難になる。さらに、昨今では、取引コンテンツ単位が小口化し、例えば音楽コンテンツの配信において曲目1曲のみを取り引きコンテンツとすることもある。このような場合、コンテンツの代金は、100円単位、1000円単位の小額のものとなり、これらの支払いにおいて、逐一、クレジットカード番号、あるいは銀行口座番号が要求されるという取引形態は、コンテンツの流通を妨げる一因ともなっている。

【0021】また、上述の(4)電子マネーの利用については、現状ではまだ試用段階であり、その利用形態が確立されておらず、一般に普及するには至っていないのが現状である。

【0022】本発明は、これらの状況に鑑みてなされたものであり、ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツ利用権の販売において、クレジットカード番号、あるいは銀行口座番号、電子マネー等を利用せず、簡易な方法、構成の情報取引システムおよび情報取引方法、並びにプログラム提供媒体を提供することを目的とする。

【0023】

【課題を解決するための手段】本発明は、上記課題を解決するためになされたものであり、本発明の第1の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有し、前記ユーザ機器は、通信手段または記憶媒体メディアを介して取得した暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記通信手段を介して前記コンテンツ利用権管理手段に送信する構成を有し、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ

鍵を前記通信手段を介して前記ユーザ機器に送信する構成を有することを特徴とする情報取引システムにある。

【0024】さらに、本発明の情報取引システムの一実施態様において、前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成を有することを特徴とする。

【0025】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させる構成としたことを特徴とする。

【0026】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式としたことを特徴とする。

【0027】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供する構成としたことを特徴とする。

【0028】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権管理手段は、前記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信する構成を有することを特徴とする。

【0029】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権管理手段は、同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供する構成を有し、前記データベースには、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定した構成を有することを特徴とする。

【0030】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売する構成としたことを特徴とする。

【0031】さらに、本発明の情報取引システムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード

毎に、コンテンツ鍵の提供回数を記録する構成を有することを特徴とする。

【0032】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントする構成を有することを特徴とする。

【0033】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定する構成としたことを特徴とする。

【0034】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定する構成を有することを特徴とする。

【0035】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードは、コンテンツ識別データ、コンテンツ利用権識別カードのカード識別データ、およびコンテンツ利用権識別カード中のデータの改竄を検証するためのチェックデータを含むことを特徴とする。

【0036】さらに、本発明の情報取り引きシステムの一実施態様において、前記チェックデータは、コンテンツ利用権識別カードを発行または管理する機関による電子署名データであることを特徴とする。

【0037】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権識別カードのカード識別データは、コンテンツ利用権識別カードの流通経路を判別可能なカード識別データであることを特徴とする。

【0038】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定する構成であることを特徴とする。

【0039】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信する構成であることを特徴とする。

【0040】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信する構成であることを特徴とする。

【0041】さらに、本発明の情報取り引きシステムの一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信する構成であることを特徴とする。

【0042】さらに、本発明の第2の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器と、前記ユーザ機器に通信手段を介して接続され、前記暗号化コンテンツの復号用のコンテンツ鍵を通信手段を介して提供するコンテンツ利用権管理手段とを有する情報取り引きシステムにおける情報取り引き方法において、暗号化コンテンツを利用するために必要となるコンテンツ利用権識別データを通信手段を介することなくオフラインでユーザに提供されるコンテンツ利用権識別カードから取得して前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、前記コンテンツ利用権管理手段において、前記ユーザ機器から受信したコンテンツ利用権識別データに基づいて該コンテンツの復号可能なコンテンツ鍵を前記通信手段を介して前記ユーザ機器に送信するステップと、を有することを特徴とする情報取り引き方法にある。

【0043】さらに、本発明の情報取り引き方法の一実施態様において、前記暗号化コンテンツをユーザに提供するコンテンツプロバイダまたはサービスプロバイダは、前記コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得することを特徴とする。

【0044】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにデータを隠した状態で流通させることを特徴とする。

【0045】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、記録された前記コンテンツ利用権識別データが外部から観察できないようにスクラッチカード形式であることを特徴とする。

【0046】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、暗号化コンテンツを格納したメディアに同梱して、ユーザに提供することを特徴とする。

【0047】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前

記コンテンツ利用権識別カードに関する管理データを格納するデータベースを有し、前記データベースには、前記コンテンツ利用権識別カードの対応するコンテンツ識別データ、および前記コンテンツ利用権識別カードのカード識別データを含み、前記コンテンツ利用権管理手段は、前記ユーザから受信したコンテンツ利用権識別データに基づいて、対応コンテンツの復号用のコンテンツ鍵を抽出して前記ユーザ機器に対して送信することを特徴とする。

【0048】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、同一のコンテンツ利用権識別カードに記録された同一のコンテンツ利用権識別データに基づいて、複数回、同一のコンテンツ鍵を提供し、前記データベースに、コンテンツ利用権識別カード毎のコンテンツ鍵提供許容回数を設定することを特徴とする。

【0049】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権識別カードは、前記コンテンツ鍵提供許容回数に応じた価格設定をしてユーザに対して販売することを特徴とする。

【0050】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記データベースに、前記コンテンツ利用権識別カード毎のコンテンツ鍵の提供回数を記録することを特徴とする。

【0051】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザを識別するユーザ識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ識別データに基づいて、ユーザの利用回数をカウントすることを特徴とする。

【0052】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記データベース中のユーザ識別データに基づいてユーザの利用回数をカウントするとともに利用回数に応じたポイントをユーザに対して付与し、該ポイントに基づいてユーザに対する特典を設定することを特徴とする。

【0053】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段の前記データベースは、前記コンテンツ利用権識別カード毎に、コンテンツ鍵の提供を受けたユーザ機器を識別するユーザ機器識別データを有し、前記コンテンツ利用権管理手段は、前記ユーザ機器識別データに基づいて、コンテンツ鍵の送信可否を判定することを特徴とする。

【0054】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器から受信したコンテンツ利用権識別データ中のチェックデータの検証処理を実行してコンテンツ利用権識別データの改竄の有無を判定することを特徴とする。

る。

【0055】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器との相互認証処理を実行して、認証が成立した場合にのみ、コンテンツ鍵を認証されたユーザ機器に対して送信することを特徴とする。

【0056】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を暗号化して送信することを特徴とする。

【0057】さらに、本発明の情報取り引き方法の一実施態様において、前記コンテンツ利用権管理手段は、前記ユーザ機器に対して送信するコンテンツ鍵を前記ユーザ機器との相互認証処理時に生成するセッション鍵を用いて暗号化して送信することを特徴とする。

【0058】さらに、本発明の第3の側面は、コンテンツプロバイダまたはサービスプロバイダから暗号化コンテンツを取得して、該暗号化コンテンツを復号して利用するユーザ機器におけるコンテンツ情報取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、オフラインでユーザに提供されるコンテンツ利用権識別カードに記録されたコンテンツ利用権識別データを前記ユーザ機器から前記通信手段を介して前記コンテンツ利用権管理手段に送信するステップと、前記コンテンツ利用権管理手段から受信したコンテンツ鍵に基づいて暗号化コンテンツを復号処理するステップと、を有することを特徴とするプログラム提供媒体にある。

【0059】本発明の第3の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MO、DVDなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0060】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0061】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【0062】

【実施例】図2に本発明の情報取り引きシステムに使用されるユーザ端末であるデータ処理装置の一実施例に係る構成ブロック図を示す。データ処理装置は、記録再生器300と記録デバイス400とを主要構成要素とする。

【0063】記録再生器300は、例えばパーソナル・コンピュータ（PC：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器300は、図2に示すように、記録再生器300における暗号処理時の記録デバイス400との通信制御を含む統括的制御を実行する制御部301、暗号処理全般を司る記録再生器暗号処理部302、記録再生器に接続される記録デバイス400と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ303、DVDなどのメディア500から少なくともデータの読み出しを行う読み取り部304、外部とデータの送受信を行う通信部305を有する。

【0064】記録再生器300は、制御部301の制御により記録デバイス400に対するコンテンツデータのダウンロード、記録デバイス400からのコンテンツデータ再生を実行する。記録デバイス400は、記録再生器300に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、EEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成される外部メモリ402を有する。

【0065】記録再生器300は、図2の左端に示す記憶媒体、DVD、CD、FD、HDDに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部304、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部305を有し、外部からコンテンツを入力する。

【0066】記録再生器300は、暗号処理部302を有し、読み取り部304または通信部305を介して外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいはコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。暗号処理部302は、暗号処理部302全体を制御する制御部306、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ307、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部308から構成されている。

【0067】制御部301は、例えば、記録再生器300と通信部305を介して接続されたコンテンツ利用管理センタ（図3以下で説明）と暗号処理部302の相互認証処理における仲介制御、セッション鍵で暗号化されて送付されるコンテンツ鍵の暗号処理部302における

復号処理における仲介制御、さらに記録デバイス400が装着された際に記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信したり、あるいは、記録再生器暗号処理部302の暗号／復号化部308と記録デバイス暗号処理部401の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。

【0068】暗号処理部302は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部306、内部メモリ307、暗号／復号化部308を有する。

【0069】暗号処理制御部306は、記録再生器300において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、コンテンツ利用管理センタ（図3以下で説明）との相互認証処理、記録再生器300と記録デバイス400との間で実行される相互認証処理の制御、記録再生器暗号処理部302の暗号／復号化部308において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関する暗号処理の実行命令等、暗号処理全般に関する制御を行なう。

【0070】内部メモリ307は、記録再生器300において実行される相互認証処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは記録再生器の識別データ等を格納する。記録再生器の識別データは、コンテンツ利用管理センタ（図3以下で説明）との相互認証処理等において必要となる。また、後段で説明するが、コンテンツ利用管理センタのデータベース中に登録されるデータとして利用される。

【0071】暗号／復号化部308は、内部メモリ307に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいは記録デバイス400に格納されたコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、データの検証、乱数の発生などの処理を実行する。

【0072】ここで、記録再生器暗号処理部302の内部メモリ307は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【0073】記録再生器300は、これらの暗号処理機能の他に、中央演算処理装置（メインCPU：Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108、AV

処理部109、入力インタフェース110、PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112を備えている。

【0074】中央演算処理装置（メインCPU：Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108は、記録再生器300本体の制御系として機能する構成部であり、主として記録再生器暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU：Central Processing Unit）106は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部109へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【0075】RAM107は、CPU106における各種処理用の主記憶メモリとして使用され、メインCPU106による処理のための作業領域として使用される。ROM108は、メインCPU106で起動されるOS等を立ち上げるための基本プログラム等が格納される。

【0076】AV処理部109は、具体的には、例えばMPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【0077】入力インタフェース110は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU106に出力する。メインCPU106は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

【0078】PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

【0079】また、メインCPU106は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス400に記憶する際の制御も行なう。この処理の際には、記憶データを制御部301に転送し、制御部301は必要に応じて暗号処理部302にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス400に格納する。

【0080】記録デバイス400は、好ましくは記録再生器300に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス400は暗号処理部401、外部メモリ402を有する。

【0081】記録デバイス暗号処理部401は、記録再生器300からのコンテンツデータのダウンロード、または記録デバイス400から記録再生器300へのコン

テンツデータの再生処理時等における記録再生器300と記録デバイス400間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、記録再生器300の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。外部メモリ402は、前述したように、例えばEEPROM、フラッシュメモリ等からなる不揮発メモリ、ハードディスク、電池つきRAMなどによって構成されコンテンツデータを格納する。

【0082】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツを提供するコンテンツプロバイダ、あるいはコンテンツの利用権を管理するコンテンツ利用権販売センタは、提供コンテンツを暗号化して、CD、DVD等のメディア、あるいはネットワークを介してユーザに提供する。さらに、CD、DVD等のメディアを介してコンテンツを流通させる場合は、コンテンツ利用権を証明する識別子を記入したカード（以下、コンテンツ利用権識別カード）を外部からは観察できないように密封してメディアに同梱して販売する。コンテンツ利用権識別カードは、識別子が外部から観察できないようにメディアパッケージ内に密封しておく。例えばスクラッチカード等のような形態を採用してもよい。

【0083】また、ネットワークを介してコンテンツを配信する場合は、コンテンツ利用権を証明する識別子を記入したカード、すなわちコンテンツ利用権識別カードは、オンラインで取り引きすることなく、オフライン、すなわち店舗等を経由してコンテンツ利用権識別カードのみをコンテンツとは別に販売する。この場合においてもコンテンツ利用権識別カードは、外部からは観察できないようにパッケージ内に密封したり、スクラッチカード等のような形態とする。

【0084】図3に、ユーザ端末と、コンテンツプロバイダと、コンテンツ利用権管理センタ間において実行されるコンテンツと、コンテンツ利用権識別カードと、コンテンツ利用権（復号鍵として利用されるコンテンツ鍵）の流通形態を説明する図を示す。

【0085】図3において、ユーザ（ユーザ端末）601は、例えば図2で説明した記録再生器である。さらに、ユーザ端末601は、ユーザ個人の所有するパーソナルコンピュータ、ゲーム機器、あるいは駅、コンビニ等の共同スペースに設置され不特定多数が利用可能な端末であってもよい。

【0086】音楽、画像、ゲームプログラム等、各種コンテンツを利用したいユーザは、ユーザ端末601を利用して、コンテンツプロバイダ602、603、604から、ネットワーク607を介して暗号化されたコンテンツの配信を受けたり、あるいはメディア606を介してコンテンツを入手する。さらに、コンテンツ購入者は、コンテンツの入手に併せてコンテンツ利用権識別カ

ードを購入、受領する。

【0087】コンテンツ利用権識別カードは、ユーザ（ユーザ端末）601がコンテンツの利用権を取得するための識別子が記録されたカードである。すなわち暗号化コンテンツの復号鍵を取得するために必要な識別子が記録されたカードである。このコンテンツ利用権識別カードは、暗号化コンテンツの配布ルートがDVD、CD等のメディアを介した形態である場合は、メディアに同梱する形態とし、また、ネットワークを介したコンテンツ配信の場合は、独立してコンテンツ利用権識別カードを配布、あるいは販売する。なお、メディアを介したコンテンツ配布の場合においても、コンテンツ利用権識別カードはメディアと同梱とすることなく、別個に独自の流通ルートで配布するようにしてもよい。いずれの場合も、コンテンツ利用権識別カードは、流通経路上では、外部から識別子データが観察できないように密封構成、例えばスクラッチ式のカードとして配布あるいは販売する。

【0088】暗号化コンテンツをユーザに提供するコンテンツプロバイダ602、603、604は、コンテンツ利用権識別カードのユーザに対する提供に応じてコンテンツ利用料金を取得する構成とすることで、ユーザからのオンラインによる料金徴収の取り引きを省略することができる。なお、コンテンツ利用権識別カードのユーザに対する提供に応じた対価の配分は、コンテンツプロバイダ、コンテンツ利用権管理センタ、さらにコンテンツ利用権識別カードを販売した店舗等の間で適宜配分するようにしてもよい。

【0089】コンテンツ利用権識別カードに記録される識別データの例を図4に示す。図4に示すように、識別データには、利用対象となるコンテンツを識別するコンテンツ識別子（ID）と、シリアル番号、電子署名が記録されている。コンテンツ識別子（ID）はユーザがコンテンツプロバイダからメディアまたはネットワークを介して入手した利用予定のコンテンツを識別するデータである。シリアル番号は、コンテンツ利用権識別カード毎の番号であり、個々のコンテンツ利用権識別カードを識別可能な番号となっている。電子署名は、コンテンツの利用権を管理する例えばコンテンツ利用管理センタ605（図3参照）の署名鍵によって、コンテンツID、シリアル番号に対して生成された署名データであり、コンテンツID、シリアル番号の改竄を防止するために付加されている。電子署名は、コンテンツ利用権識別カードを発行または管理する機関によって行われる。なお、図4では、電子署名をコンテンツ利用権識別カードに記録されるチェックデータとして使用しているが、電子署名を用いない、例えばチェックサムのような簡易なチェックデータを付与する構成としてもよい。

【0090】図3に戻り、ユーザ端末と、コンテンツプロバイダと、コンテンツ利用権管理センタ間において実

行されるコンテンツと、コンテンツ利用権識別カードと、コンテンツ利用権（復号鍵）の流通形態の説明を続ける。

【0091】暗号化コンテンツをメディア606またはネットワーク607を介して受領したユーザ（ユーザ端末）601は、図4で説明したデータ構成を持つコンテンツ利用権識別カードをメディア606に併せて、あるいは別ルートで購入、受領する。

【0092】コンテンツ利用権識別カードを購入、受領したユーザ601は、コンテンツ利用権識別カードに記録された、コンテンツID、シリアル番号、電子署名から構成される識別データをコンテンツ利用権管理センタ605にネットワーク607を介して送信する。

【0093】コンテンツ利用権管理センタ605は、発行済みのコンテンツ利用権識別カードに関する情報をデータベースにより管理しており、例えばシリアル番号で識別されるコンテンツ利用権識別カードに対応するコンテンツの復号鍵の配布がすでに実行されているか否か等のデータを管理している。コンテンツ利用権管理センタ605は、ユーザから受領したコンテンツ利用権識別カードに記録された、コンテンツID、シリアル番号、電子署名から構成される識別データを正当であるかどうかを判定し、さらに、コンテンツを識別し、また、すでに鍵を配信しているかどうか等をチェックする。

【0094】これら各種のチェックの後、コンテンツ利用権管理センタ605がユーザに対してコンテンツ利用権を配布すると判定した場合は、ユーザに対する復号鍵（コンテンツ鍵）の配布を行なう。なお、コンテンツ鍵の配布は、ネットワークでの通信の安全性を考慮して暗号化して送付することが望ましく、例えばユーザ端末との相互認証処理後に共有するセッション鍵で暗号化して送信する。鍵を受信したユーザは、受領した暗号化コンテンツ鍵をセッション鍵で復号して、復号したコンテンツ鍵を用いて暗号化コンテンツの復号処理を実行して、コンテンツを利用可能とする。

【0095】コンテンツ利用管理センタ605が有するコンテンツ利用権識別カードに関するデータベースを図5に示す。データベースには、利用対象となるコンテンツを識別するコンテンツ識別子（ID）と、シリアル番号、利用権（復号鍵）の販売回数、利用権の購入者情報、その他の情報が含まれる。コンテンツ識別子（ID）と、シリアル番号は、前述の図4において説明したコンテンツ利用権識別カード中のデータに対応するデータである。利用権（復号鍵）の販売回数は、後段でさらに説明するが、1つのコンテンツ利用権識別カードを再販することによって、複数回、利用権を販売した場合に、その回数を記録したものである。購入者情報は、購入者の識別データを記録している。その他の情報としては、シリアル番号に対応するコンテンツ利用権識別カードの再販可能性の有無、さらに再販可能である場合の再

販可能回数が記録されている。再販については、後段で説明する。

【0096】図5に示す例においては、コンテンツ利用権識別カードに応じて再販可能なカードであるもの（上段2つ）と、再販不可能なもの（中段2つ）と、再販可能なカードにおいて最大販売回数が規定されたもの（下段2つ）のそれぞれがデータベース中に設定されている。

【0097】図6に本発明の情報取り引きシステムを構成する、コンテンツ利用権管理センタと、コンテンツプロバイダと、ユーザ端末の構成ブロック図を示す。ユーザ端末900は、前述の図2で説明した記録再生器300と同様であり、同一構成部には同一符号を付してある。記録再生器300の各構成要素については、図2において説明したので、説明を省略する。

【0098】図6において、コンテンツ利用権管理センタ700は、ユーザ端末900と通信を実行するための通信部703、通信制御を含む統括的制御を実行する制御部701、暗号処理全般を司る暗号処理部702、前述の図5で説明したコンテンツ利用権識別カードの管理データを格納したデータベース704、コンテンツの復号処理に用いるコンテンツ鍵を格納するコンテンツ鍵格納メモリ705を有している。暗号処理部702は、ユーザ端末900との相互認証処理、セッション鍵生成処理、セッション鍵によるコンテンツ鍵の暗号化処理を実行する。

【0099】また、コンテンツプロバイダ800は、メディア500、またはネットワーク等の通信手段600を介して暗号化コンテンツをユーザに対して供給する構成を持ち、コンテンツを格納したコンテンツデータベース804、コンテンツの暗号処理を実行する暗号処理部802、ユーザ端末との通信を実行する通信部803、通信制御を含む統括的制御を実行する制御部801を有する。なお、図6に示すコンテンツプロバイダの構成は一例であり、例えばメディアのみの供給を行なうプロバイダであれば通信手段を必要としない。

【0100】また、図6では、コンテンツ管理センタと、コンテンツプロバイダとを独立した手段として示してあるが、両機能を併せ持った1つの手段でコンテンツ管理センタとコンテンツプロバイダの両機能を提供するように構成としてもよい。

【0101】図6に示す構成において実行される各処理手続きの詳細について説明する。まず、図4で説明したコンテンツ利用権識別カードは、コンテンツ利用権管理センタ700がコンテンツプロバイダ800からのコンテンツ配布に伴って作成する。コンテンツ管理センタ700は、新たに配布されるコンテンツにコンテンツ識別子を付与し、さらに、発行するコンテンツ利用権識別カード毎にシリアル番号を付与し、さらに、これらのコンテンツ識別子とシリアル番号に対して電子署名を生成し

て、図4で説明したデータを有するコンテンツ利用権識別カードを生成し、これをコンテンツプロバイダの供給するコンテンツ、例えばメディアに同梱してユーザに提供する。あるいはコンテンツプロバイダがネットワーク配信によりコンテンツを提供する場合は、コンテンツとは別ルートで、例えば特定の店舗においてコンテンツ利用権識別カードを販売、配布する。

【0102】なお、ここでは、コンテンツ利用権管理センタ700がコンテンツ利用権識別カードを作成する例を説明するが、コンテンツプロバイダがコンテンツ利用権識別カードを作成して、作成したコンテンツ利用権識別カード情報をコンテンツ利用管理センタに提供し、その後の利用権配布手続きをコンテンツ利用権管理センタ700に任せる構成としてもよい。

【0103】コンテンツ利用権識別カードの構成データである電子署名データの生成処理方法の例の1つとして共通鍵暗号方式におけるDESを用いた例を説明する。なお、本発明においては、DES以外にも、同様の共通鍵暗号方式における処理として例えばFEAL（Fast Encipherment Algorithm：NTT）、AES（Advanced Encryption Standard：米国次期標準暗号）等を用いることも可能である。

【0104】一般的なDESを用いた電子署名の生成方法を図7を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを8バイト単位に分割する（以下、分割されたメッセージをM1、M2、・・・、MNとする）。そして、初期値（Initial Value（以下、IVとする））とM1を排他的論理和する（その結果をI1とする）。次に、I1をDES暗号化部に入れ、鍵（以下、K1とする）を用いて暗号化する（出力をE1とする）。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する（出力E2）。以下、これを繰り返す、全てのメッセージに対して暗号化処理を施す。最後に出てきたENが電子署名になる。この値は一般にはメッセージ認証符号（MAC（Message Authentication Code））と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをCBC（Cipher Block Chaining）モードと呼ぶ。このMAC値の検証時には、検証者が生成時と同様の方法でMAC値を生成し、同一の値が得られた場合、検証成功とする。

【0105】本発明の情報取り引きシステムにおいて使用されるコンテンツ利用権識別カードには、図4を用いて説明したようにコンテンツIDとシリアル番号が含まれ、これらが検証対象のメッセージに対応する。従って、これらのデータ、あるいはこれらのデータに基づいて生成されるデータを図7に示すDES暗号処理部に入力するメッセージとして電子署名を生成する。

【0106】次に、公開鍵暗号方式を用いた電子署名の

生成方法を図8を用いて説明する。図8に示す処理は、EC-D SA ((Elliptic Curve Digital Signature Algorithm) 、 IEEE P1363/D3) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptography (以下、 ECC と呼ぶ)) を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えば RSA 暗号 ((Rivest, Shamir, Adleman) など (ANSI X9.31)) を用いることも可能である。

【 0107 】 図8の各ステップについて説明する。ステップ S1 において、 p を標数、 a、 b を楕円曲線の係数 (楕円曲線 : $y^2 = x^3 + ax + b$) 、 G を楕円曲線上のベースポイント、 r を G の位数、 K s を秘密鍵 ($0 < K s < r$) とする。ステップ S2 において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【 0108 】 ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、 MD4、 MD5、 SHA-1 などが用いられる場合もあるし、 DES-CBC が用いられる場合もある。この場合は、最終出力値となる MAC (チェック値 : ICV に相当する) がハッシュ値となる。

【 0109 】 続けて、ステップ S3 で、乱数 u ($0 < u < r$) を生成し、ステップ S4 でベースポイントを u 倍した座標 V (X_v, Y_v) を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【 0110 】

【 数 1 】 $P = (X_a, Y_a), Q = (X_b, Y_b), R = (X_c, Y_c) = P + Q$ とすると、 $P \neq Q$ の時 (加算) 、
 $X_c = \lambda^2 - X_a - X_b$

$Y_c = \lambda \times (X_a - X_c) - Y_a$
 $\lambda = (Y_b - Y_a) / (X_b - X_a)$

P=Q の時 (2倍算) 、

$X_c = \lambda^2 - 2X_a$
 $Y_c = \lambda \times (X_a - X_c) - Y_a$
 $\lambda = (3(X_a)^2 + a) / (2Y_a)$

【 0111 】 これらを用いて点 G の u 倍を計算する (速度は遅いが、最もわかりやすい演算方法として次のように行う。 G、 2×G、 4×G、…を計算し、uを2進数展開して1が立っているところに対応する $2^i \times G$ (G を i 回2倍算した値) を加算する (i は u の LSB から数えた時のビット位置)) 。

【 0112 】 ステップ S5 で、 $c = X_v \bmod r$ を計

算し、ステップ S6 でこの値が0になるかどうか判定し、0でなければステップ S7 で $d = [(f + cKs) / u] \bmod r$ を計算し、ステップ S8 で d が0であるかどうか判定し、dが0でなければ、ステップ S9 で c および d を電子署名データとして出力する。仮に、r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【 0113 】 ステップ S6 において、cが0であった場合、ステップ S3 に戻って新たな乱数を生成し直す。同様に、ステップ S8 で d が0であった場合も、ステップ S3 に戻って乱数を生成し直す。

【 0114 】 次に、公開鍵暗号方式を用いた電子署名の検証方法を、図9を用いて説明する。ステップ S11 で、M をメッセージ、p を標数、a、b を楕円曲線の係数 (楕円曲線 : $y^2 = x^3 + ax + b$) 、G を楕円曲線上のベースポイント、r を G の位数、G および $Ks \times G$ を公開鍵 ($0 < Ks < r$) とする。ステップ S12 で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップ S13 で、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。次に、ステップ S14 で $h1 = d \bmod r$ を計算し、ステップ S15 で $h1 = fh \bmod r$ 、 $h2 = ch \bmod r$ を計算する。

【 0115 】 ステップ S16 において、既に計算した h1 および h2 を用い、点 $P = (X_p, Y_p) = h1 \times G + h2 \times Ks \times G$ を計算する。電子署名検証者は、公開鍵 G および $Ks \times G$ を知っているため、図8のステップ S4 と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップ S17 で点 P が無限遠点かどうか判定し、無限遠点でなければステップ S18 に進む (実際には、無限遠点の判定はステップ S16 でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、λが計算できず、 $P + Q$ が無限遠点であることが判明している) 。ステップ S18 で $X_p \bmod r$ を計算し、電子署名データ c と比較する。最後に、この値が一致していた場合、ステップ S19 に進み、電子署名が正しいと判定する。

【 0116 】 電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【 0117 】 ステップ S12 において、電子署名データ c または d が、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップ S20 に進む。また、ステップ S17 において、点 P が無限遠点であった場合もステップ S20 に進む。さらにまた、ステップ S18 において、 $X_p \bmod r$ の値が、電子署名データ c と一致していなかった場合にもステップ S20 に進む。

【 0118 】 ステップ S20 において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成

したのではないことがわかる。

【0119】本発明の情報取り引きシステムにおいて使用されるコンテンツ利用権識別カードは、コンテンツ利用権管理センタ700、あるいはコンテンツプロバイダ800において、電子署名を作成し、コンテンツ利用権管理センタにおいて、電子署名の検証を行なう。コンテンツプロバイダ800において電子署名を作成し、コンテンツ利用権管理センタ700において、電子署名の検証を行なう場合は、コンテンツ利用権管理センタ700は、電子署名の作成を行なったコンテンツプロバイダ800に対応する電子署名検証用の鍵を保持する構成とする。

【0120】図6に戻って、コンテンツ利用権配布手続きについての説明を続ける。図6におけるユーザ端末900は、コンテンツを取得するとともに、あるいは別ルートで購入したコンテンツ利用権識別カードに記録された識別データを通信手段600を介してコンテンツ利用権管理センタ700に送信する。コンテンツ利用権管理センタ700は、ユーザ端末900から送信されてきたコンテンツ利用権識別カードのデータについて、署名検証を例えば上述の手法に従って実行してデータの改竄チェックを実行する。

【0121】コンテンツ利用権管理センタ700は、署名検証によりデータ改竄がないことを検証した後、ユーザから送信された識別データ中のコンテンツIDとシリアル番号に一致するデータ(図5参照)をデータベース704から抽出する。ここで対応するデータの販売回数が0であれば、そのシリアル番号に対応するコンテンツ利用権識別カードに関してはまだ利用権(コンテンツ鍵)の配布を一度も行っていない、すなわち初回の配布であることが確認され、コンテンツ鍵をコンテンツ鍵格納メモリ705から取り出してユーザに対して送信する。なお、コンテンツ鍵は、暗号化して送信することが好ましい。ユーザに対するコンテンツ鍵の送信とともに、データベース704の対応データの販売回数を「1」に設定する。

【0122】なお、コンテンツ利用権管理センタ700からユーザ端末900に対するコンテンツ鍵送信は、ネットワークを介した通信における安全性を考慮して前述したようにコンテンツ鍵を暗号処理部702において暗号化処理した後、送信することが望ましい。コンテンツ鍵の暗号化には、共通鍵暗号方式による共通鍵を使用した暗号化処理、あるいは公開鍵暗号方式によるコンテンツ利用権管理センタの秘密鍵による暗号化処理、あるいは、ユーザ端末900と、コンテンツ利用権管理センタ700との相互認証処理を実行して生成するセッション鍵を用いて暗号化処理する方法等がある。相互認証処理について、以下、説明する。

【0123】共通鍵暗号方式を用いた相互認証方法を、図10を用いて説明する。図10において、共通鍵暗号

方式としてDESを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図10において、A、Bは一方が図6におけるユーザ端末900に対応し、他方がコンテンツ利用権管理センタ700に対応する。

【0124】まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、ID(b)がM3に相当し、初期値:IV=0としたときの出力E1、E2、E3が暗号文となる。

【0125】これを受信したBは、受信データを鍵Kabで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵Kabで復号化し、乱数Raを得る。次に、暗号文E2を鍵Kabで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を鍵Kabで復号化し、その結果とE2を排他的論理和し、ID(b)を得る。こうして得られたRa、Rb、ID(b)の内、RbおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0126】次にBは、認証後に使用するセッション鍵(Session Key(以下、Ksesとする))を生成する(生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで鍵Kabを用いて暗号化し、Aに返送する。

【0127】これを受信したAは、受信データを鍵Kabで復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたRb、Ra、Ksesの内、RbおよびRaが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ksesは、認証後の秘密通信のための共通鍵として利用される。

【0128】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0129】次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図11を用いて説明する。図11において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図11において、まずBが、64ビットの乱数Rbを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数Raおよび標数pより小さい乱数Akを生成する。そして、ベースポイン

トGをAk倍した点 $A_v = A_k \times G$ を求め、Ra、Rb、Av (X座標とY座標) に対する電子署名A. Sigを生成し、Aの公開鍵証明書とともにBに返送する。ここで、RaおよびRbはそれぞれ64ビット、AvのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図8で説明したので、その詳細は省略する。

【0130】公開鍵証明書は、公開鍵暗号方式における認証局 (CA: Certificate Authority) が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0131】図12に示す公開鍵証明書の例を示す。図12に示すように公開鍵証明書には、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前 (ユーザID)、証明書利用者の公開鍵並びに電子署名を含む。

【0132】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図8で説明した処理フローが適用される。

【0133】認証局は、図12に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布 (これをリボケーション: Revocationと呼ぶ) を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0134】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図9で説明したのでその詳細は省略する。

【0135】図11に戻って説明を続ける。Aの公開鍵証明書、Ra、Rb、Av、電子署名A. Sigを受信したBは、Aが送信してきたRbが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名A. Sigを検証する。電子署

名の検証方法は図9で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0136】次に、Bは、標数pより小さい乱数Bkを生成する。そして、ベースポイントGをBk倍した点 $B_v = B_k \times G$ を求め、Rb、Ra、Bv (X座標とY座標) に対する電子署名B. Sigを生成し、Bの公開鍵証明書とともにAに返送する。

【0137】Bの公開鍵証明書、Rb、Ra、Bv、電子署名B. Sigを受信したAは、Bが送信してきたRaが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B. Sigを検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0138】両者が認証に成功した場合には、Bは $B_k \times A_v$ (Bkは乱数だが、Avは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要) を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する (共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0139】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0140】コンテンツ利用権管理センタ700は、このような相互認証処理において、生成したセッション鍵を用いて、コンテンツ鍵を暗号化して、ユーザ端末900に対して送信する。

【0141】暗号化されたコンテンツ鍵を受信したユーザ端末900は、暗号処理部302において、認証処理の際に生成したセッション鍵を用いてコンテンツ鍵の復号処理を実行する。復号処理によって得られるコンテンツ鍵は、コンテンツ利用権識別カードに記録されたコンテンツ、すなわちメディア500または通信手段600を介して受領した暗号化コンテンツを復号可能なコンテンツ鍵であり、ユーザは、このコンテンツ鍵を利用して暗号化コンテンツの復号処理を実行し、コンテンツを利用可能なデータに復号する。

【0142】このように、本発明の情報取り引きシステムおよび情報取り引き方法に従えば、コンテンツプロバイダ、コンテンツ販売会社等は、クレジットカード、あるいは銀行口座指定によるオンラインでの決済システムを構築する必要がなく、コンテンツの利用料金をコンテンツ利用権識別カードの販売料金としてコンテンツ利用

権識別カードの流通ルートを紹介して回収することが可能となる。従って、クレジットカード、または銀行口座を持たないユーザによるコンテンツの利用が容易になる。

【0143】なお、上述した説明においては、コンテンツプロバイダがコンテンツの作成、配信を一括して行なう構成として説明したが、コンテンツの作成をコンテンツプロバイダが実行して、コンテンツプロバイダの作成したコンテンツの暗号化処理、配信サービスをコンテンツプロバイダからコンテンツの提供を受けたサービスプロバイダが実行する構成としてもよい。

【0144】[コンテンツ利用権の再販] 上述した例では、コンテンツ利用権識別カードに基づくコンテンツ鍵の配布は1回のみ行われる構成であったが、本発明の情報取り引きシステムおよび情報取り引き方法におけるコンテンツ利用権識別カードを用いることにより、コンテンツ利用権識別カードを取得したユーザか他のユーザに同一のコンテンツ利用権識別カードを譲渡することにより、コンテンツ利用権識別カードを譲渡された他のユーザが、そのコンテンツ利用権識別カードに基づいてコンテンツ鍵をコンテンツ利用権管理センタから新たに取得する構成が実現される。以下、この構成について説明する。

【0145】図13にコンテンツ利用権識別カードをユーザ間において譲渡し、異なるユーザが同一のコンテンツ利用権識別カードに基づいてコンテンツ鍵を取得する構成を説明する図を示す。図13においてユーザ（ユーザ端末）1301はコンテンツプロバイダ1303から暗号化コンテンツを取得し、コンテンツ利用権識別カードを購入する（図の（1）で示す手続き）。

【0146】ユーザ（ユーザ端末）1301は、前述した手続きに従って、コンテンツ利用権識別カードの識別データをコンテンツ利用権管理センタ1304に送信（図の（2）で示す手続き）し、コンテンツ鍵を受領（図の（3）で示す手続き）してコンテンツを復号してコンテンツの利用を行なう。ユーザ（ユーザ端末）1301は、暗号化コンテンツの格納されたメディアとコンテンツ利用権識別カードをユーザ（ユーザ端末）1302に譲渡（図の（4）で示す手続き）する。

【0147】ユーザ（ユーザ端末）1302は、譲渡されたコンテンツ利用権識別カードの識別データをコンテンツ利用権管理センタ1304に送信（図の（5）で示す手続き）し、コンテンツ鍵を受領（図の（6）で示す手続き）してコンテンツを復号してコンテンツの利用を行なう。

【0148】なお、この場合のコンテンツ利用料金のユーザ（ユーザ端末）1302からの回収は、従来のクレジットカード、銀行口座指定による料金回収が可能である。あるいは、コンテンツ利用権識別カードに設定した再販可能回数に応じたコンテンツ利用権識別カード価格を設定して最初のユーザに販売するようにしてもよい。

例えば再販不可能なコンテンツ利用権識別カード、すなわち1つのコンテンツ鍵の取得が可能なコンテンツ利用権識別カードが1000円としたとき、1回再販可能なコンテンツ利用権識別カード、すなわち初回を合わせて2回、コンテンツ鍵を取得可能なコンテンツ利用権識別カードを2000円、2回再販可能なコンテンツ利用権識別カード、すなわち初回を合わせて3回、コンテンツ鍵を取得可能なコンテンツ利用権識別カードを3000円で販売する設定とすれば、コンテンツ利用権識別カードを譲渡されたユーザもオンライン決済手続き等が不要となる。なお、2回、3回等の複数回のコンテンツ鍵取得権を有するカードについては割引を行なって販売する構成としてもよい。

【0149】コンテンツ利用権管理センタ1304は、このようなコンテンツ利用権識別カードの再販可能情報は、先に図5を用いて説明したコンテンツ利用権管理センタデータベースにおいて管理している。図5から理解されるように発行されたコンテンツ利用権識別カードはシリアル番号が付与され、個々のカードが識別可能であり、それらについて再販可能性、最大可能回数Nが設定されている。図5の例では、上段の2つのコンテンツ利用権識別カードは再販ができない、すなわち1回限りコンテンツ鍵を取得可能なコンテンツ利用権識別カードである。中段の2つのコンテンツ利用権識別カードは、再販が可能なコンテンツ利用権識別カードであり、再販回数が規定されていないカードである。下段の2つのカードは、再販回数がNに設定されており、N回までコンテンツ鍵をコンテンツ利用権管理センタ1304から取得可能な鍵として設定されている。

【0150】コンテンツ利用権管理センタ1304は、ユーザからコンテンツ利用権識別カードデータを受信した際、図5に示すデータベース中の対応データを抽出して、その設定情報に従って、コンテンツ鍵の送信、非送信を決定する。例えばN回までコンテンツ鍵をコンテンツ利用権管理センタ1304から取得可能な鍵として設定されたコンテンツ利用権識別カードデータの受信を受けた場合には、販売回数をチェックし、Nを超えない範囲においてのみコンテンツ鍵を送信する。コンテンツ利用権管理センタ1304がコンテンツ鍵の送信を行なった場合は、データベースの販売回数を1インクリメントする。

【0151】また、図5に示すデータ中には、購入者情報が記録されており、コンテンツ利用権管理センタ1304は、最初にコンテンツ利用権識別カードを購入したユーザ情報を、そのコンテンツ利用権識別カードのシリアル番号に対応付けて登録し、そのコンテンツ利用権識別カードに基づく複数回のコンテンツ購入依頼があった場合に、購入回数に応じたポイントを登録ユーザに付与して、例えば異なるコンテンツ購入、あるいはコンテンツ利用権識別カード購入料金をポイントに応じて割引

くサービスを提供する。

【0152】なお、コンテンツ利用権識別カードに付与されるシリアル番号は、流通経路毎に分類する構成とすることが好ましい。この構成とすることにより、シリアル番号に基づいて、その流通経路が判別可能となり、コンテンツ利用権識別カードの改竄等により不正なシリアル番号を持つコンテンツ利用権識別カードが市場に流通することを防止することができる。

【0153】さらに、コンテンツ利用権管理センタ1304は、管理データとして、ユーザの同一性判定情報、ユーザ機器の機器情報を持つことにより、同一ユーザからの利用の場合にポイントを付与したり、また、同一機器からのコンテンツ鍵取得要求には、繰り返し応じる等の処理が可能となる。

【0154】このデータベース例を図14に示す。図14に示すデータベースには、利用対象となるコンテンツを識別するコンテンツ識別子(ID)と、シリアル番号、利用権(復号鍵)の販売回数、利用権の購入者情報、ユーザ識別データ、ユーザ機器識別データ、その他の情報が含まれる。コンテンツ識別子(ID)と、シリアル番号、利用権(復号鍵)の販売回数、利用権の購入者情報、その他の情報は、前述の図5において説明したと同様のデータである。

【0155】ユーザ識別データは、コンテンツ利用権識別カードデータを送信したユーザから取得する、例えばユーザID+パスワード、あるいは指紋、虹彩、声紋等、ユーザ固有のバイオメトリックス情報を登録しておく、これらの情報をコンテンツ利用権管理センタ1304がユーザからのコンテンツ利用権識別カードデータ受信に際して受信してユーザ同一性を判定し、同一ユーザの利用であった場合には、ユーザに対するポイントを付与する。

【0156】また、ユーザ機器識別データは、ユーザの使用機器のIDを登録して、同一ユーザ機器からのコンテンツ鍵取得要請であった場合には、コンテンツ鍵の繰り返し送信を許容する構成とすることができる。なお、ユーザ使用機器の同一性判定は、前述の図10、11の相互認証処理において実行可能である。

【0157】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0158】

【発明の効果】上述したように、本発明の情報取り引きシステムおよび情報取り引き方法に従えば、コンテンツプロバイダ、コンテンツ販売会社等は、クレジットカード、あるいは銀行口座指定によるオンラインでの決済シ

ステムを構築する必要がなく、また、ユーザ間において同一のコンテンツ利用権識別カードの譲渡が可能となり、同一の識別に基づいて複数回コンテンツ鍵を送受信することが可能となり、コンテンツの利用が促進される。コンテンツプロバイダ、コンテンツ販売会社等は、コンテンツの利用料金をコンテンツ利用権識別カードの販売料金としてコンテンツ利用権識別カードの流通ルートを通じて回収することが可能となる。従って、クレジットカード、または銀行口座を持たないユーザによるコンテンツの利用が容易になる。

【図面の簡単な説明】

【図1】従来の暗号化コンテンツ利用形態を説明する図である。

【図2】本発明の情報取り引きシステムにおいて利用可能なデータ処理装置の構成を示す図である。

【図3】本発明の情報取り引きシステムにおけるコンテンツ、コンテンツ利用権識別カードの流通形態を説明する図である。

【図4】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードのデータ構成を示す図である。

【図5】本発明の情報取り引きシステムにおけるコンテンツ利用権管理センタのデータベースのデータ構成を示す図である。

【図6】本発明の情報取り引きシステムにおけるユーザ端末、コンテンツ利用権管理センタ、コンテンツプロバイダの構成を説明する図である。

【図7】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名生成について説明する図である。

【図8】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名生成について説明する図である。

【図9】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの署名検証について説明する図である。

【図10】本発明の情報取り引きシステムにおける相互認証処理について説明する図である。

【図11】本発明の情報取り引きシステムにおける相互認証処理について説明する図である。

【図12】本発明の情報取り引きシステムにおける相互認証処理において使用される公開鍵証明書の構成について説明する図である。

【図13】本発明の情報取り引きシステムにおけるコンテンツ利用権識別カードの再販構成を説明する図である。

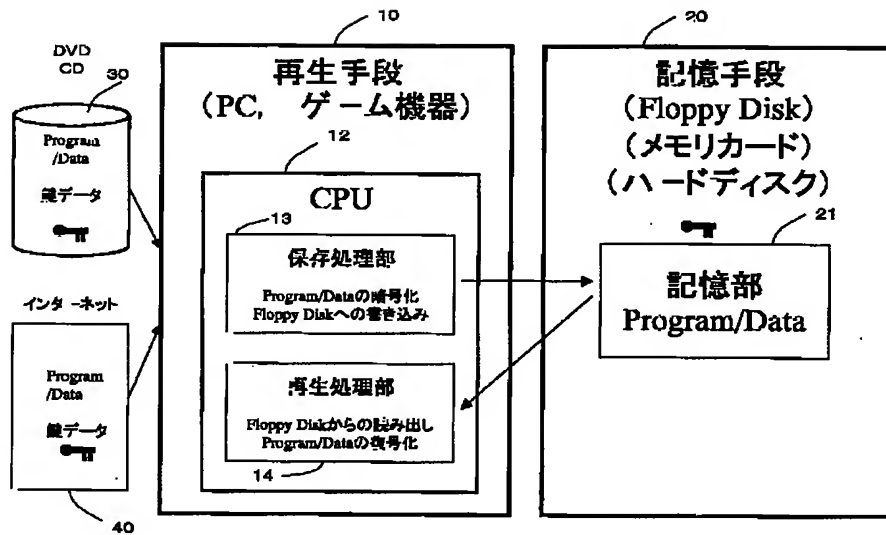
【図14】本発明の情報取り引きシステムにおけるコンテンツ利用権管理センタのデータベースのデータ構成を示す図である。

【符号の説明】

106 メインCPU

- | | | | |
|-----|--------------|---------------|---------------|
| 107 | RAM | 550 | 通信手段 |
| 108 | ROM | 601 | ユーザ端末 |
| 109 | AV処理部 | 602, 603, 604 | コンテンツプロバイダ |
| 110 | 入力処理部 | 605 | コンテンツ利用権管理センタ |
| 111 | PIO | 606 | メディア |
| 112 | SIO | 607 | ネットワーク |
| 300 | 記録再生器 | 700 | コンテンツ利用権管理センタ |
| 301 | 制御部 | 701 | 制御部 |
| 302 | 暗号処理部 | 702 | 暗号処理部 |
| 303 | 記録デバイスコントローラ | 703 | 通信部 |
| 304 | 読み取り部 | 704 | データベース |
| 305 | 通信部 | 705 | コンテンツ鍵格納メモリ |
| 306 | 制御部 | 800 | コンテンツプロバイダ |
| 307 | 内部メモリ | 801 | 制御部 |
| 308 | 暗号/復号化部 | 802 | 暗号処理部 |
| 400 | 記録デバイス | 803 | 通信部 |
| 401 | 暗号処理部 | 804 | データベース |
| 402 | 外部メモリ | 900 | ユーザ端末 |
| 500 | メディア | | |

【図1】

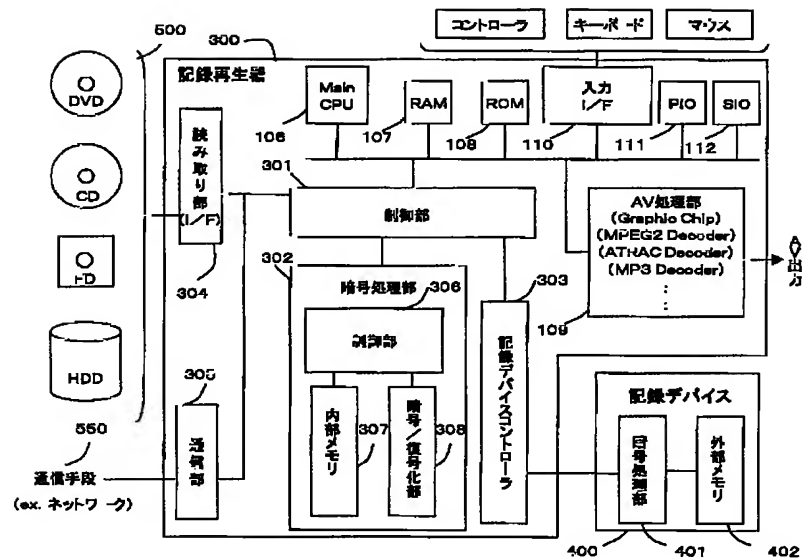


【図4】

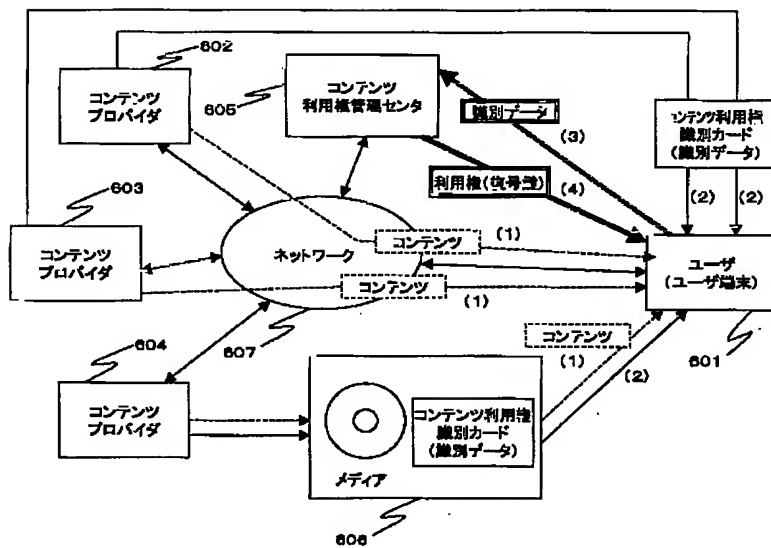
識別データ構成

コンテンツID	シリアル番号	電子署名
01234567	0000123	34251748

【図2】



【図3】

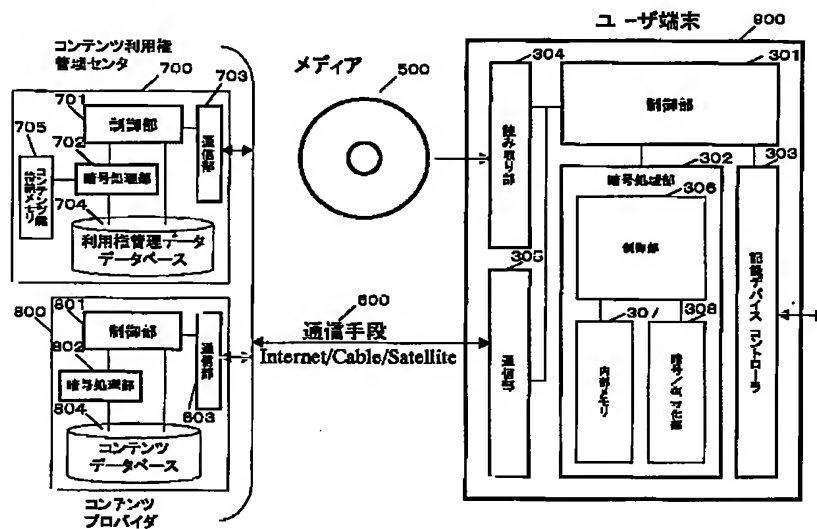


【図5】

コンテンツ利用権管理センタデータベース

コンテンツID	シリアル番号	販売回数	購入者情報	その他
01234567	0000123	0		再販不可能
01234567	0000124	0		再販不可能
99999999	0000125	1	ACD22222	再販可能
99999999	0000126	2	BBF33333	再販可能
22222222	0000127	5		最大販売回数 N
22222222	0000128	N-1		最大販売回数 N

【図6】

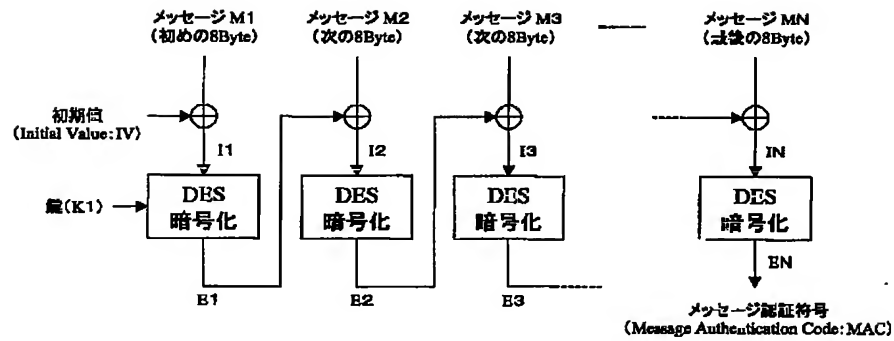


【図14】

コンテンツ利用権管理センタデータベース

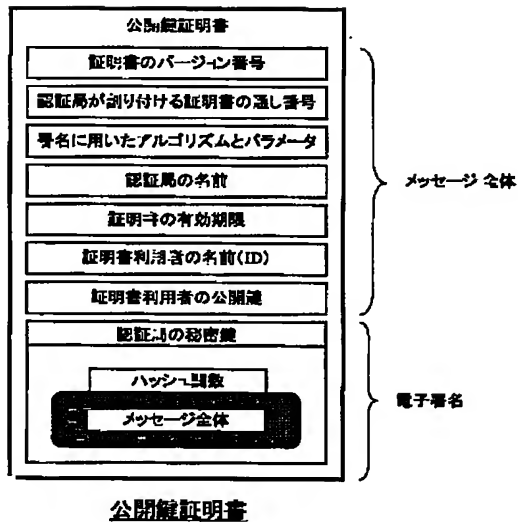
コンテンツID	シリアル番号	販売回数	購入者情報	ユーザ識別データ	ユーザ機器識別データ	その他
01234567	0000123	0				再販不可能
01234567	0000124	0				再販不可能
99999999	0000125	1	ACD22222	BCD38432	ABA23255	再販可能
99999999	0000126	2	BBF33333	BBB28756	BBC37854	再販可能
22222222	0000127	5	CBD36578	CDA15683	BBA36529	最大販売回数 N
22222222	0000128	N-1	DD28215	ABB19653	CCB35532	最大販売回数 N

【図7】



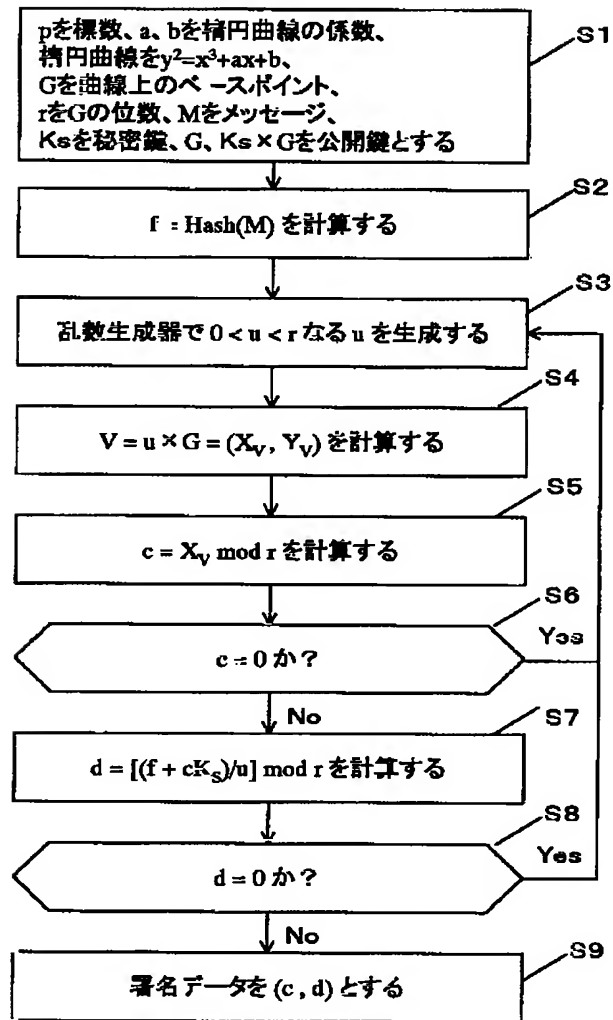
⊕ : 排他的論理和処理(8バイト単位)

【図12】



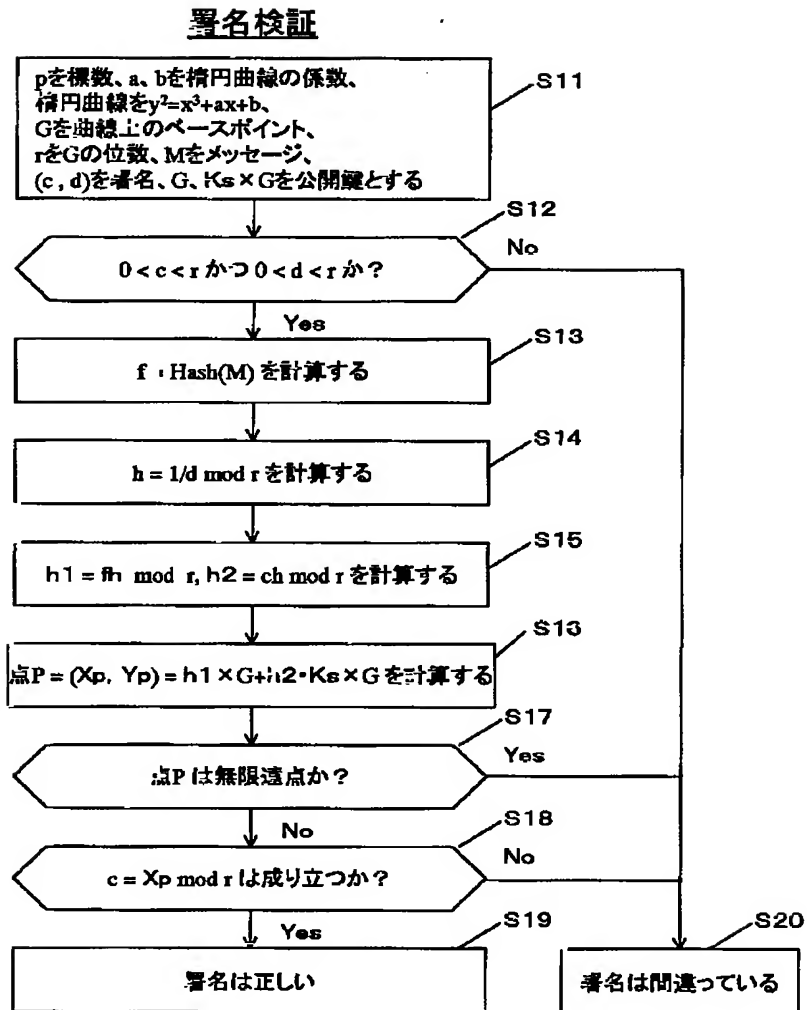
【図8】

署名生成

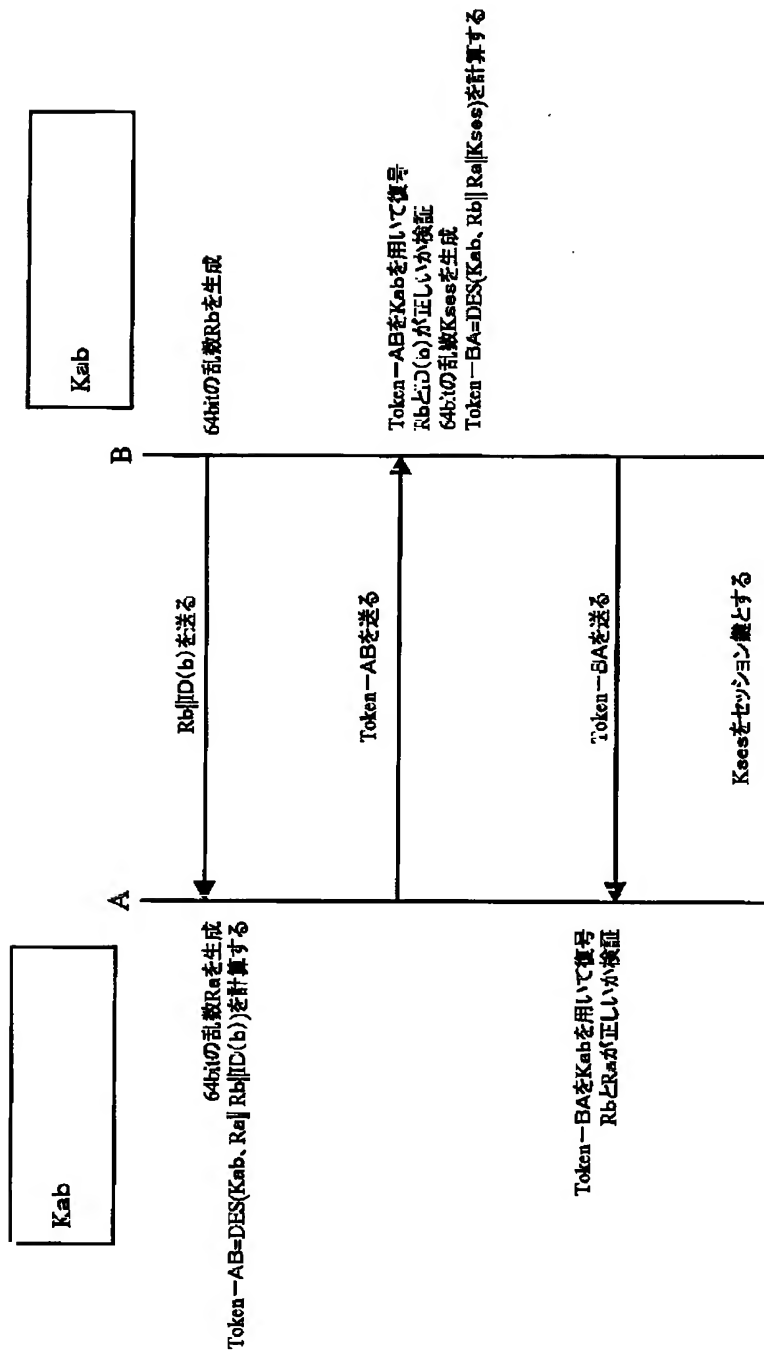


署名生成(IEEE P1363/D3)

【図9】

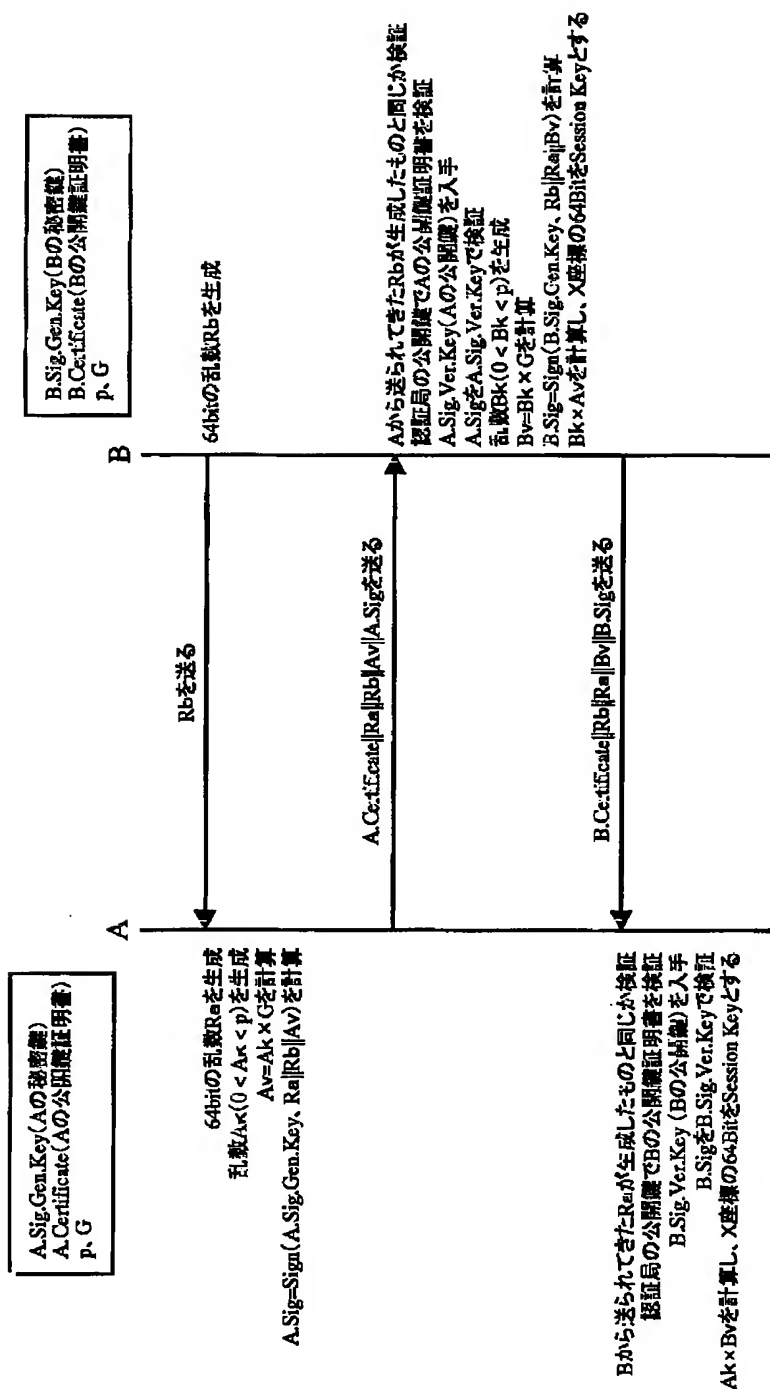


【図10】

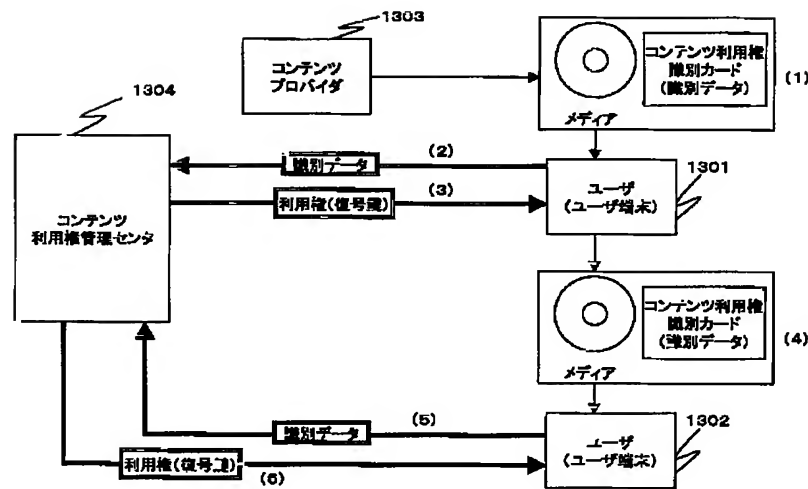


ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図11】



【図13】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	(参考)
G 0 7 F 7/08		G 0 9 C 1/00	6 4 0 B 9 A 0 0 1
17/00		H 0 4 L 9/00	6 0 1 B
G 0 9 C 1/00	6 2 0	G 0 6 F 15/21	Z E C Z
	6 4 0		3 4 0 Z
		G 0 7 F 7/08	R
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B

Fターム(参考) 3E044 BA04 DA05 DC05 DC06 DD02
 DE01
 5B017 AA06 BA07 CA15 CA16
 5B049 AA05 BB11 CC08 CC36 DD01
 DD04 DD05 EE03 EE07 EE21
 FF06 FF08 FF09 GG02 GG04
 GG07 GG10
 5B085 AE12 AE13 AE23 AE29
 5J104 AA09 AA16 EA16 JA13 JA14
 JA25 JA28 LA02 LA03 LA06
 MA06 NA02 NA12 NA33 NA37
 PA07 PA14
 9A001 CZ02 EE03 FF01 JZ76 KK60
 KK62 LL03